(2)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-132020
(43)Date of publication of application : 09.05.2003

(51)Int.Cl. G06F 15/00
G06F 13/00
H04L 9/32

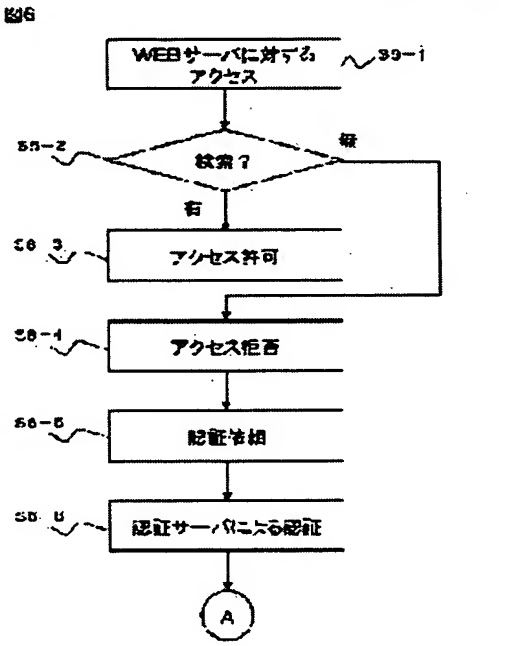
(21)Application number : 2001-329307
(22)Date of filing : 26.10.2001

(71)Applicant : CYBER SIGN JAPAN INC
(72)Inventor : KANEKO HISAHIRO

(54) ACCESS CONTROL APPARATUS, AUTHENTICATION APPARATUS AND APPARATUS RELATED TO THEM

NCS-0023

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an apparatus and a program, capable of dynamically changing access control rule.
SOLUTION: When an external terminal 20 accessing to an WEB server 16, if access has not been permitted and the access is refused, the external terminal 20 transmits an authentication request to an authentication server 18, to obtain permission. The authentication server 18 authenticates, based on the signature data included in the authentication request, if the external terminal 20 is an authorized one, and requests to a firewall to set the access control rule to permit 'access controls to be executed', included in the authentication request. The firewall 10 sets the access control rule, based on the request. Accordingly, the access control rule corresponded to a current user can be set, so that a network can be used smoothly.



LEGAL STATUS

[Date of request for examination] 21.10.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－132020
（Ｐ２００３－１３２０２０Ａ）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
G06F 15/00	330	G06F 15/00	330	A	5B085
			330	F	5B089
13/00	351	13/00	351	Z	5J104
H04L 9/32		H04L 9/00	673	D	

審査請求　未請求　請求項の数７　ＯＬ　（全10頁）

(21)出願番号　特願2001－329307(Ｐ2001－329307)

(22)出願日　平成13年10月26日(2001.10.26)

(71)出願人　500120668
日本サイバーサイン株式会社
東京都世田谷区用賀４丁目５番16号　ＴＥビル５Ｆ

(72)発明者　金子　尚浩
東京都世田谷区用賀４丁目５番16号　ＴＥビル５Ｆ　日本サイバーサイン株式会社内

(74)代理人　100109014
弁理士　伊藤　充

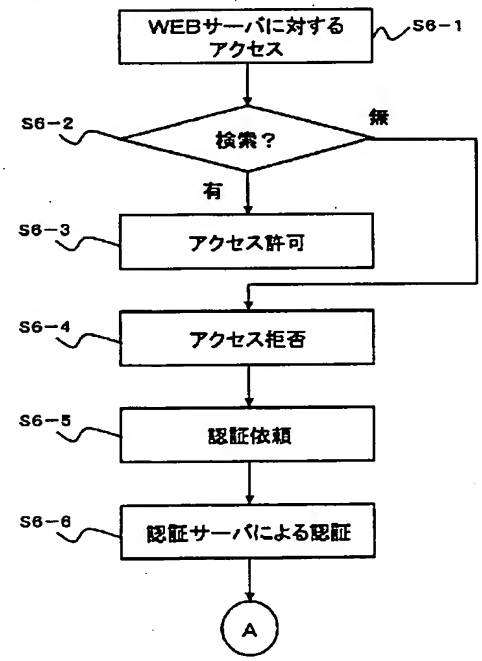
Ｆターム(参考)　5B085 AE25 BA07 BG02 BG03 BG07
5B089 GA11 GA21 GB02 HA10 JB22 KA17
5J104 AA07 KA01 KA16 NA05 PA07

(54)【発明の名称】アクセス制御装置及び認証装置及びそれらに関連する装置

(57)【要約】
【課題】　アクセス制御ルールを動的に変更しうる装置やプログラムを提供することである。
【解決手段】　外部端末２０がＷＥＢサーバ１６に対してアクセスを行おうとする。このアクセスが許可されていない場合は、アクセス拒否された場合、外部端末２０は、許可を得るために認証サーバ１８に認証依頼を送信する。認証サーバ１８は、認証依頼中の署名データに基づき認証し、正当な者であれば、認証依頼中に含まれていた「実行したいアクセス内容」を許可するアクセス制御ルールを、ファイアーウォール１０に設定するように依頼する。この依頼に基づき、ファイアーウォール１０がアクセス制御ルールを設定する。この結果、現在の使用者に対応したアクセス制御ルールが設定できるので、円滑なネットワークの利用が可能である。

NCS－0023

図6



1

【特許請求の範囲】

【請求項１】　第１ネットワークと、第２ネットワーク間のアクセスを制御するアクセス制御装置において、

アクセス制御ルールが格納されたアクセス制御テーブルと、

前記第１ネットワークから第２ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、

前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、

前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、

バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、

を含むことを特徴とするアクセス制御装置。

【請求項２】　ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御装置において、

アクセス制御ルールが格納されたアクセス制御テーブルと、

前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、

前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、

前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、

バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、

を含むことを特徴とするアクセス制御装置。

【請求項３】　認証すべき人のバイオメトリックデータが予め格納されている認証テーブルと、

実行したい希望アクセス内容とバイオメトリックデータとを含む認証依頼を受信した場合に、前記バイオメトリックデータを前記認証テーブル中から検索する検索手段と、

前記検索手段が前記バイオメトリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手段と、

を含むことを特徴とする認証装置。

2

【請求項４】　ネットワーク上の所定のホストにアクセスしようとした際に、そのアクセスが拒否された場合に、所定の認証装置に認証依頼を送信する認証依頼手段、

を含み、

前記認証依頼には、自己を示す識別子と、自己が実行しようとする希望アクセス内容と、自己を示すデータであるバイオメトリックデータと、が含まれることを特徴とするネットワークアクセス装置。

【請求項５】　第１ネットワークと、第２ネットワーク間のアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記第１ネットワークと、前記第２ネットワーク間のアクセスを制御するアクセス制御装置として動作させるためのプログラムにおいて、

前記コンピュータに、

前記第１ネットワークから第２ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手順と、

前記検索手順において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手順と、

前記検索手順において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手順と、

バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手順と、

を実行させることを特徴とするアクセス制御プログラム。

【請求項６】　ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記ネットワークと、前記ネットワークに接続された前記ホストとのアクセスを制御するアクセス制御装置として動作させるプログラムにおいて、

前記コンピュータに、

前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手順と、

前記検索手順において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手順と、

前記検索手順において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセス

を実行させるアクセス制御手順と、
バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手順と、
を実行させることを特徴とするアクセス制御プログラム。

【請求項７】　認証すべき人のバイオメトリックデータが予め格納されている認証テーブルを備えたコンピュータを、認証装置として動作させるプログラムにおいて、前記コンピュータに、
実行したい希望アクセス内容とバイオメトリックデータとを含む認証依頼を受信した場合に、前記バイオメトリックデータを前記認証テーブル中から検索する検索手順と、
前記検索手順において前記バイオメトリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手順と、
を実行させることを特徴とする認証プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク上のアクセスコントロールを動的に変更しうる装置及びその装置を構成するためのプログラムに関する。

【０００２】

【従来の技術】ネットワーク上の各ホスト（端末やサーバ、クライアント、ルータ等のネットワーク上の１個の主体）を識別するために、たとえばインターネットではＩＰアドレスと呼ばれるアドレスが用いられている。ネットワーク上の各ホストは、このＩＰアドレスを用いて通信の相手先を指定している。

【０００３】しかし、ネットワーク上の各ホストが自由に他のホストにアクセスできるわけではない。一般にセキュリティ上の問題や、管理上の都合により、あるホストに対するアクセスが制限されたり、あるホストからの発信が制限される場合は多い。

【０００４】このような制御をするために、ファイアーウォールやルータ、ブリッジと呼ばれる装置が使用されており、また、各ホスト毎にアクセスを制御するためにパーソナルファイアーウォールと呼ばれるプログラムも知られている。

【０００５】

【発明が解決しようとする課題】このように、ファイアーウォールやルータ、ブリッジを用いて各種のアクセス制御が実行されていたが、この制御ルールはＩＰアドレスを用いて記述される場合が多い。たとえば、ＩＰアドレス１００．１００．１００．０からＩＰアドレス１００．１００．２００．ＸＸＸに対するアクセスは認められない（ＸＸＸは任意の数）等のようなものである。

【０００６】しかし、近年、ダイヤルアップによるインターネットアクセスに代表されるように、同じＩＰアドレスが常に同じ人（や装置）に利用されるとは限らない状況が一般的になっている。このようなＩＰアドレスがダイナミックに割り当てられる状況の下では、ＩＰアドレスを用いた固定的なアクセス制御ルールだけでは実際の利用形態に対応できない場合も想定される。

【０００７】たとえば、あるＩＰアドレスは今日は課長が使用しているが、明日は部長が使用するかもしれない。この場合、課長と部長のアクセス権限が異なることも考えられるので、今日と明日で同じ固定的なアクセス制御ルールでは、実態に対処することは困難である。

【０００８】本発明は、このような課題に鑑みなされたものであり、アクセス制御ルールを動的に変更しうる装置やプログラムを提供することである。

【０００９】

【課題を解決するための手段】上記課題を解決するために、本発明は、第１ネットワークと、第２ネットワーク間のアクセスを制御するアクセス制御装置において、アクセス制御ルールが格納されたアクセス制御テーブルと、前記第１ネットワークから第２ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、を含むことを特徴とするアクセス制御装置である。

【００１０】このような構成によって、アクセス制御ルールを動的に変更等することができる。

【００１１】また、本発明は、ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御装置において、アクセス制御ルールが格納されたアクセス制御テーブルと、前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手段と、前記検索手段が前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手段と、前記検索手段が前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手段と、バイオメトリクス認証結果を第３者に渡

す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手段と、を含むことを特徴とするアクセス制御装置である。

【００１２】このような構成によって、パーソナルファイアーウォールにおいてもアクセス制御ルールを動的に変更等することができる。

【００１３】また、本発明は、認証すべき人のバイオメトリックデータが予め格納されている認証テーブルと、実行したい希望アクセス内容とバイオメトリックデータとを含む認証依頼を受信した場合に、前記バイオメトリックデータを前記認証テーブル中から検索する検索手段と、前記検索手段が前記バイオメトリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手段と、を含むことを特徴とする認証装置である。

【００１４】このような構成によって、バイオメトリックデータによる認証結果を外部に送信することができる。

【００１５】また、本発明は、ネットワーク上の所定のホストにアクセスしようとした際に、そのアクセスが拒否された場合に、所定の認証装置に認証依頼を送信する認証依頼手段、を含み、前記認証依頼には、自己を示す識別子と、自己が実行しようとする希望アクセス内容と、自己を示すデータであるバイオメトリックデータと、が含まれることを特徴とするネットワークアクセス装置である。

【００１６】このような構成によって、アクセスが拒否された場合に自動的に認証依頼を発することができる。

【００１７】以下に述べる手段は、上記装置に関する手段を、プログラムとして表現したものであり、その本質的な特徴・作用は、上記装置に関する手段と同様である。

【００１８】すなわち、本発明は、第１ネットワークと、第２ネットワーク間のアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記第１ネットワークと、前記第２ネットワーク間のアクセスを制御するアクセス制御装置として動作させるためのプログラムにおいて、　前記コンピュータに、前記第１ネットワークから第２ネットワークへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手順と、　前記検索手順において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手順と、前記検索手順において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手順と、バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手順と、を実行させることを特徴とするアクセス制御プログラムである。

【００１９】また、本発明は、ネットワークと、前記ネットワークに接続されたホストとのアクセスを制御するアクセス制御ルールが格納されたアクセス制御テーブルを備えたコンピュータを、前記ネットワークと、前記ネットワークに接続された前記ホストとのアクセスを制御するアクセス制御装置として動作させるプログラムにおいて、前記コンピュータに、前記ネットワークから前記ホストへのアクセス要求があった場合に、要求されたアクセスを、前記アクセス制御テーブルから検索する検索手順と、前記検索手順において前記アクセスを前記アクセス制御テーブルから見いだせなかった場合に、前記発信元にアクセス拒否を送信する拒否手順と、前記検索手順において前記発信元を前記アクセス制御テーブルから見いだせた場合に、前記アクセス制御テーブルに格納されたアクセス制御ルールに基づき、アクセスを実行させるアクセス制御手順と、バイオメトリクス認証結果を第３者に渡す認証サーバから、アクセス制御ルールの設定依頼が送信されてきた場合に、前記アクセス制御テーブルの内容を変更、追加又は削除するアクセス制御ルール管理手順と、を実行させることを特徴とするアクセス制御プログラムである。

【００２０】また、本発明は、認証すべき人のバイオメトリックデータが予め格納されている認証テーブルを備えたコンピュータを、認証装置として動作させるプログラムにおいて、前記コンピュータに、実行したい希望アクセス内容とバイオメトリックデータとを含む認証依頼を受信した場合に、前記バイオメトリックデータを前記認証テーブル中から検索する検索手順と、前記検索手順において前記バイオメトリックデータを前記認証テーブル中から見いだせた場合に、前記認証依頼に含まれる希望アクセス内容を許可するようなアクセス制御ルールを設定するように外部のアクセス制御装置に依頼する依頼手順と、を実行させることを特徴とする認証プログラムである。

【００２１】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【００２２】実施の形態１（ファイアーウォール）

図１には、本発明の好適な実施の形態であるファイアーウォール１０を含むネットワーク構成図が示されている。

【００２３】この図に示すように、ファイアーウォール１０は、インターネット１２と、ローカルネットワーク１４とに接続している。このローカルネットワーク１４

には、ＷＥＢサーバ１６と認証サーバ１８とが接続している。また、インターネット１２には、外部端末２０が接続している。

【００２４】このファイアーウォール１０は、請求の範囲の「アクセス制御装置」の一例に相当する。また、認証サーバ１８は、請求の範囲の「認証装置」の一例に相当する。また、外部端末２０は、請求の範囲の「ネットワークアクセス装置」の一例に相当する。

【００２５】インターネット１２側の外部端末２０からは、ローカルネットワーク１４内のアドレスは直接見えずに、ローカルネットワーク１４に対して代表となるＩＰアドレスが１個割り当てられている。この代表となるＩＰアドレスは直接的には、ファイアーウォール１０のＩＰアドレスである。

【００２６】外部端末２０からローカルネットワーク１４のＷＥＢサーバ１６にアクセスする場合には、この代表的なＩＰアドレス（ファイアーウォール１０のＩＰアドレス）にアクセスし、利用するポート番号としてたとえば８０を指定するのである。このポート番号によって、ファイアーウォール１０は、外部端末２０がＷＥＢサービスを利用したいということを知り、外部端末２０からのアクセスをＷＥＢサーバ１６に送り出すのである。

【００２７】なお、ここでは、ＷＥＢサービスのポート番号として８０を利用したが、その他のポート番号でも良い。このようにポート番号で指定することによって、ローカルネットワーク１４内の各ホストを識別している。

【００２８】ファイアーウォール１０の構成

ファイアーウォール１０の構成ブロック図が図２に示されている。この図に示すように、ファイアーウォール１０は、インターネット１２の外部端末２０からのアクセス要求を受け、その要求されたアクセスをアクセス制御テーブル２６中のアクセス制御ルールから検索する検索手段２２と、検索した結果、見いだせなかった場合にそのアクセスを拒否する拒否手段２４とが備えられている。

【００２９】また、ファイアーウォール１０は、検索手段２２が、要求されたアクセスを、アクセス制御テーブル２６中から見いだした場合に、その要求されたアクセスを実行するアクセス制御手段２８と、アクセス制御テーブル２６の内容であるアクセス制御ルールを管理するアクセス制御ルール管理手段３０とを備えている。

【００３０】本実施の形態において特徴的なことはアクセス制御テーブル２６中のアクセス制御ルールが動的に追加、変更、削除される点である。この点に関しては、後に詳述する。

【００３１】アクセス制御ルールは、一般に、認められるアクセスを記述したものであり、アクセス制御テーブル２６は複数のアクセス制御ルールを集めた表である。

【００３２】アクセス制御テーブル２６の内容を表す説明図が図３に示されている。この図に示すように、アクセス制御テーブル２６の各エントリー（すなわち、認められるアクセスを記述したアクセス制御ルール）は、発信元の情報と、発信先の情報と、から構成されている。発信元の情報とは、発信元のＩＰアドレス及びポート番号であり、発信先の情報とは、発信先のＩＰアドレス及びポート番号である。なお、この表中Ｘはいわゆるワイルドカードであり、すべての番号を表す記号である。また、表中では、ある特定の数字が記述される例を示しているが、一定の範囲、たとえば１００．１００．１００．１００～１００．１００．１００．３００のような範囲で示しても良い。ファイアーウォール１０は、この図３の表に示されていない組み合わせのアクセスを拒否する。

【００３３】なお、ファイアーウォール１０中の検索手段２２、アクセス拒否手段２４、アクセス制御手段２８、アクセス制御ルール管理手段３０は、プログラムとそのプログラムを実行するプロセッサから構成されることが好ましい。また、アクセス制御テーブル２６はハードディスク等の上に構築されることが好ましい。このプロセッサとは、請求の範囲の「コンピュータ」の一例に相当する。

【００３４】認証サーバ１８の構成

認証サーバ１８の構成ブロック図が図４に示されている。本実施の形態における認証サーバ１８は、バイオメトリックデータによって個人認証を行うサーバである。バイオメトリックデータとしては署名データを利用しているが、他のバイオメトリックデータ、たとえば指紋データや、網膜パターン等でもかまわない。

【００３５】図４に示すように、認証サーバ１８は、署名データが予め登録されている認証テーブル４０と、外部からの依頼によって認証テーブル４０を検索する検索手段４２とを備えている。また、認証サーバ１８は、ファイアーウォール１０等のアクセス制御装置に、アクセス制御ルールの調整（追加、変更、削除など）を依頼する依頼手段４４を備えている。このような構成によって、署名データによって認証された利用者が希望するアクセスを許可するようなアクセス制御ルールがファイアーウォール１０に設定される。

【００３６】なお、検索手段４２、依頼手段４４は、プログラムとこのプログラムを実行するプロセッサとから構成することが望ましい。また、認証テーブル４０はハードディスク等の上に構築することが望ましい。

【００３７】外部端末２０の構成

外部端末２０の構成ブロック図が図５に示されている。この図に示すように、外部端末２０は、ＷＥＢサーバ１６に接続し、ＷＥＢページを閲覧するためのＷＥＢ閲覧手段４６と、アクセスが拒否された場合に外部の認証サーバ１８に認証を依頼する認証依頼手段４８と、を備え

ている。

【００３８】ＷＥＢ閲覧手段４６は、いわゆるブラウザと呼ばれるプログラム（及びそれを実行するプロセッサ）で構成することが望ましい。このプログラムを用いてＷＥＢサーバ１６が提供するＷＥＢページをディスプレイ４９に表示する。認証依頼手段４８も、プログラムとそれを実行するプロセッサから構成されることが望ましい。したがって典型的には、この外部端末２０はブラウザなどのプログラムがインストールされたコンピュータで実現される。もちろん、ＰＤＡ（Personal Digital Assistant）や携帯電話等、インターネット１２に接続しうる装置であればそのような装置でもかまわない。

【００３９】動作

以下、本実施の形態におけるアクセスの処理の流れをフローチャートに基づき説明する。図６、図７には、この動作を表すフローチャートが示されている。

【００４０】まず、ステップＳ６－１においては、外部端末２０がＷＥＢサーバ１６に対してアクセスを行おうとする。このアクセスは、ＷＥＢ閲覧手段４６によって実行される。

【００４１】ステップＳ６－２においては、このアクセス要求は、ファイアーウォール１０に受信され、ファイアーウォール１０がこのアクセスがアクセス制御テーブルに記載されているか検索が行われる。この検索は、検索手段２２によって実行される。検索は、発信元と発信先のＩＰアドレス及びポート番号が、アクセス制御テーブル２６中に記載されているか否かを検査することによって実行される。記載されていれば、それはアクセスが許可されていることを意味し、ステップＳ６－３に処理が移行する。一方、記載されていない場合は、ステップＳ６－４に処理が移行する。

【００４２】ステップＳ６－３においては、アクセスが許可されているので、そのままアクセスを認める。すなわち、ＷＥＢサーバ１６（ポート番号：８０）に外部端末２０からの送信データを転送するのである。

【００４３】ステップＳ６－４においては、許可されていない者からのアクセスであると判断し、アクセス拒否を外部端末２０に送信する。この拒否動作は、アクセス拒否手段２４によって実行される。

【００４４】ステップＳ６－５においては、アクセスを拒否された外部端末２０が許可を得るために認証サーバ１８に認証依頼を送信する。認証依頼手段４８がこの動作を実行する。本実施の形態において特徴的なことは、この認証依頼中に、外部端末２０の利用者のＩＤと利用者の署名データとが含まれていることである。さらに、認証依頼中には、実行したいアクセスの内容を含むことができる。

【００４５】なお、このＩＤは、請求の範囲の「識別子」の一例である。また、署名データは請求の範囲中の「バイオメトリックデータ」の一例である。また、実行したいアクセスの内容は、請求の範囲中の「希望アクセス内容」に該当する。この実行したいアクセスの内容は、自己のＩＰアドレスやポート番号、及びアクセスの相手先のＩＰアドレスやポート番号が含まれる。また、実行したいアクセスの内容中に、アクセスを開始したい時刻や、終了したい時刻を含めても良い。

【００４６】実行したいアクセスの内容（希望アクセス内容）は、サーバ側のポリシーとの組み合わせで、実際のアクセスルールがファイアーウォール１０に適用される。なお、サーバ側とは、認証サーバ１８（認証装置）、ファイアーウォール１０（アクセス制御装置のいずれかを言う。しかし、認証サーバ１８がポリシーを持つのが一般的であろう。たとえば、外部端末２０（クライアント）から社員Ａのアカウントで役員ＢのＰＣに対するアクセス許可を希望した場合でも、認証装置側に役員のＰＣには役員自身が認証を行わないとアクセスを許可しないようにポリシー設定されている場合その希望は許可されない。極端に言えば、外部端末２０（クライアント）側から希望が出されなくても認証サーバ１８（認証装置）側に設定されたポリシーにしたがってファイアーウォール１０（アクセス制御装置）にルールを適用することも好ましい。

【００４７】この認証サーバ１８のポート番号はたとえば９９９９に設定されており、誰でもアクセスが許可されているポートとして設定されている。

【００４８】ステップＳ６－６においては、認証サーバ１８が上記認証依頼を受信し、認証動作を実行する。具体的には、認証サーバは１８の検索手段４２が、認証依頼中の署名データを認証テーブル４０から検索する。その後図７のステップＳ７－１に処理が移行する。

【００４９】ステップＳ７－１において、認証依頼中の署名データと同一人による署名データであると認められるほど近似した署名データが認証テーブル４０中に見いだされた場合には、ステップＳ７－２に処理が移行し、アクセス制御ルールの調整が行われる。一方、同一人による署名データと認められる署名データが認証テーブル４０中になかった場合には、ステップＳ７－４に処理が移行する。

【００５０】ステップＳ７－２においては、認証依頼中に含まれていた「実行したいアクセス内容」を許可するアクセス制御ルールを、ファイアーウォール１０に設定するように依頼が行われる。この依頼は、依頼手段４４が実行する。

【００５１】ステップＳ７－３においては、上記依頼に基づき、ファイアーウォール１０がアクセス制御ルールをアクセス制御テーブル２６に登録する。

【００５２】このように、本実施の形態によれば、動的にアクセス制御テーブル２６中のアクセス制御ルールが調整される。すなわち、一つのＩＰアドレスを複数人が共有している場合でも、現在の使用者に対応したアクセ

ス制御ルールが設定できるので、円滑なネットワークの利用が可能である。

【００５３】アクセス制御ルールが変更された後は、外部端末２０からＷＥＢサーバ１６に対するアクセスが許可される。具体的には、図６におけるステップＳ６－１、Ｓ６－２、Ｓ６－３の流れの処理が実行される。

【００５４】ステップＳ７－４においては、認証拒否（失敗）が外部端末２０に送信される。

【００５５】このように、本実施の形態によれば、バイオメトリックデータ（署名データ）により、本人を認証し、これに基づいてアクセス制御ルールを動的に変更する仕組みが実現されている。

【００５６】アクセス制御ルールの調整

上述したように動的に調整（変更、追加、削除）されたアクセス制御ルールは、所定期間経過した場合、又は、アクセスが所定期間以上なかった場合に、元に戻すことが望ましい。これによって、一時的なアクセス制御ルールの調整に対応することができるのである。

【００５７】実施の形態２Ａ（ルータ装置）

実施の形態１では、請求の範囲の「アクセス制御装置」の例としてファイアーウォール１０を説明したが、ファイアーウォールの代わりにルータ装置を利用することも好ましい。この場合のアクセス制御ルールには、ルーティング（Routing）・ルールを含むことができる。また、ルータは、２つのネットワーク間に設けられるだけでなく、複数のネットワークに接続しうるものであるので、このルーティング・ルールも一般的には複数のネットワーク間のルーティングに関するルールである。

【００５８】このようにルータ装置によれば、ＩＰアドレスの利用者のバイオメトリックデータによって、ルーティング・ルールを含めたアクセス制御ルールを動的に変更することができる。

【００５９】なお、請求の範囲における「アクセス制御ルール」はアクセスに関するルールであればどのようなルールでもかまわない。たとえば、グローバルＩＰアドレスとローカルアドレスとの変換を行うルールでも良い。

【００６０】実施の形態２Ｂ（ブリッジ）

また、ファイアーウォール１０の代わりに、ブリッジと呼ばれる装置を利用することも好ましい。このブリッジはネットワークを接続する装置として知られているが、この接続状況を表すルールがアクセス制御ルールとなる。このブリッジも請求の範囲の「アクセス制御装置」の一例に相当する。

【００６１】この接続状況を表すルールを利用者のバイオメトリックデータによって動的に変化させることが可能である。

【００６２】実施の形態３（認証サーバの一体化）

なお、実施の形態１では、ファイアーウォール１０と認証サーバ１８は別体に構成したが、一体に構成することも好ましい。この場合、ファイアーウォール１０中に認証サーバ１８が組み込まれる形態となる。

【００６３】このような形態を実現するためには、ファイアーウォール１０中に、認証サーバ１８の動作を実行するプログラムを組み込み、またハードディスク等の上に認証テーブル４０を構築するのが好ましい。

【００６４】この一体に構成した場合は、請求の範囲の「ネットワーク装置」の一例に相当し、その中のファイアーウォール１０に該当する機能は請求の範囲の「アクセス制御ユニット」に、認証サーバ１８に該当する機能は請求の範囲の「認証ユニット」に、それぞれ相当する。

【００６５】実施の形態４（ホストベースファイアーウォール）

上記の例では、ネットワーク間のファイアーウォール１０について説明したが、１個のローカル端末５０とインターネット１２との間に設けられるファイアーウォールにアクセス制御ルールの動的な変更の動作を持たせることも好ましい。このような１個のローカル端末５０に関してアクセスの制御を行ってその外部端末を保護する装置を、本特許明細書では、ホストベースファイアーウォール５２と呼ぶ。

【００６６】このようなホストベースファイアーウォール５２を中心としたネットワーク構成図が図８に示されている。この図に示すように、ローカル端末５０は、ホストベースファイアーウォール５２を介してインターネット１２に接続する構成である。このローカル端末５０上では、ＨＴＴＰプログラムが起動しており、ローカル端末５０は、ＷＥＢサーバ１６の動作を実行している。そして、外部端末２０から、このホストベースファイアーウォール５２を介してＷＥＢサーバ１６（ローカル端末５０）に接続しようとする。

【００６７】ホストベースファイアーウォール５２の構成は、図２に示したファイアーウォール１０とほぼ同様である。異なる点は、ネットワーク間のアクセス制御ではなく、ネットワークとローカル端末との間のアクセス制御を行う点と、アクセス制御ルール管理手段に対する依頼が、ローカルネットワークではなくインターネット１２側から来る点である。その他の点は図２の構成と同様である。

【００６８】また、本実施の形態における動作も、上記図６及び図７に示した動作と同様である。

【００６９】本実施の形態によれば、ローカル端末５０を保護するホストベースファイアーウォール５２のアクセス制御ルールをバイオメトリックデータの一つである署名データによる認証を介して動的に変更することができる。したがって、同じＩＰアドレスを複数人が共同で使用する場合等においても、ローカル端末５０を効果的に保護することができる。

【００７０】なお、このホストベースファイアーウォー

ル５２も、請求の範囲の「アクセス制御装置」の一例に相当する。

【００７１】実施の形態５（端末との一体化）

実施の形態４では形式的には、ハードウェアでホストベースファイアーウォール５２を構成した。しかし、このホストベースファイアーウォール５２をローカル端末５０上で稼働するプログラムで実現しても良い。

【００７２】実施の形態６Ａ（認証サーバとの一体化）

なお、実施の形態４では、ホストベースファイアーウォール５２と認証サーバ１６は別体に構成したが、一体に構成することも好ましい。この場合、ファイアーウォール１０中に認証サーバ１８が組み込まれる形態となる。

【００７３】このような形態を実現するためには、ホストベースファイアーウォール５２中に、認証サーバ１６の動作を実行するプログラムを組み込み、またハードディスク等の上に認証テーブル４０を構築するのが好ましい。

【００７４】このような構成は、請求の範囲の「ネットワーク装置」の一例に相当する。

【００７５】実施の形態６Ｂ（端末及び認証サーバとの一体化）

なお、実施の形態６Ａのようにホストベースファイアーウォール５２と認証サーバ１８とを一体に構成する場合も、これらをローカル端末５０上で稼働するプログラムで実現しても良い。

【００７６】すなわち、ローカル端末５０中に、ホストベースファイアーウォール５２の動作を実行するプログラムを組み込むと共に、ハードディスク等の上にアクセス制御テーブル２６を構築するのである。さらに、ローカル端末５０中に、認証サーバ１８の動作を実行するプログラムを組み込み、またハードディスク等の上に認証テーブル４０を構築するのである。このような構成によって、ローカル端末５０上で稼働するプログラムを用いて、ホストベースファイアーウォール５２及び認証サーバ１８を実現することができる。

【００７７】

【発明の効果】以上述べたように、本発明によれば、バイオメトリックデータによる認証に基づきアクセス制御ルールを動的に変更等することができるので、アドレスを利用する者の変更等に迅速に対処することができる。

【図面の簡単な説明】

【図１】本発明の好適な実施の形態１のファイアーウォールを含むネットワーク構成図である。

【図２】ファイアーウォールの構成ブロック図である。

【図３】アクセス制御テーブルの内容を表す説明図である。

【図４】認証サーバの構成ブロック図である。

【図５】外部端末の構成ブロック図である。

【図６】本実施の形態におけるアクセスの処理の流れを表すフローチャートである。

【図７】本実施の形態におけるアクセスの処理の流れを表すフローチャートである。

【図８】ホストベースファイアーウォールを中心としたネットワーク構成図である。

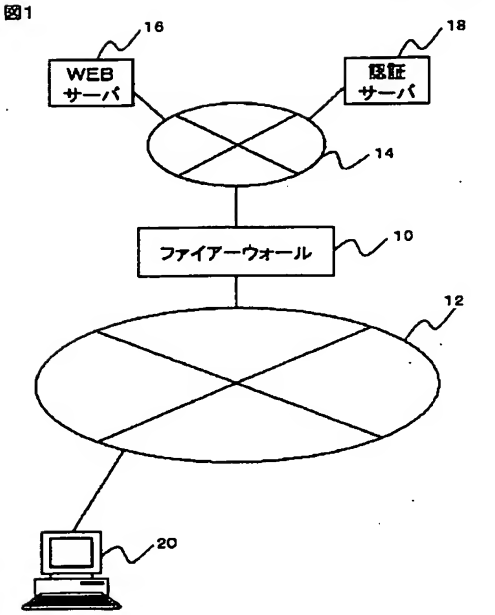
【符号の説明】

１０　ファイアーウォール
１２　インターネット
１４　ローカルネットワーク
１６　ＷＥＢサーバ
１８　認証サーバ
２０　外部端末
２２　検索手段
２４　アクセス拒否手段
２６　アクセス制御テーブル
２８　アクセス制御手段
３０　アクセス制御ルール管理手段
４０　認証テーブル
４２　検索手段
４４　依頼手段
４６　ＷＥＢ閲覧手段
４８　認証依頼手段
４９　ディスプレイ
５０　ローカル端末
５２　ホストベースファイアーウォール

【図１】

NCS－0023

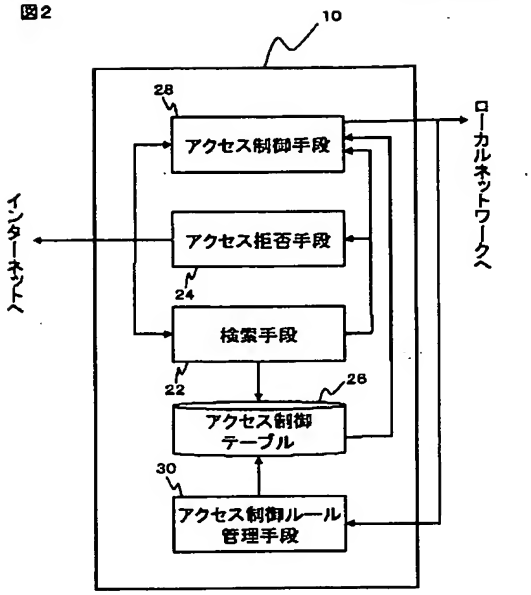
図1



【図２】

NCS－0023

図2



【図３】

NCS－0023

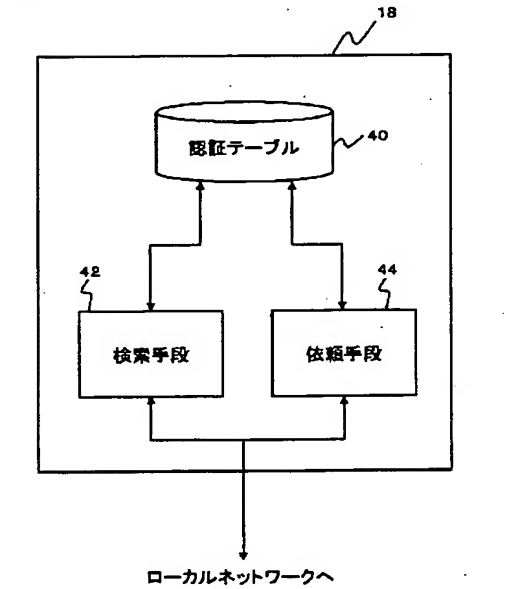
図3

発信元		発信先	
IPアドレス	ポート番号	IPアドレス	ポート番号
100.100.100.0	5	100.100.200.XXX	XX
100.100.XXX.XXX	XX	100.100.200.0	80
XXX.XXX.XXX.XXX	XX	100.100.200.0	9999
⋮	⋮	⋮	⋮

【図４】

NCS－0023

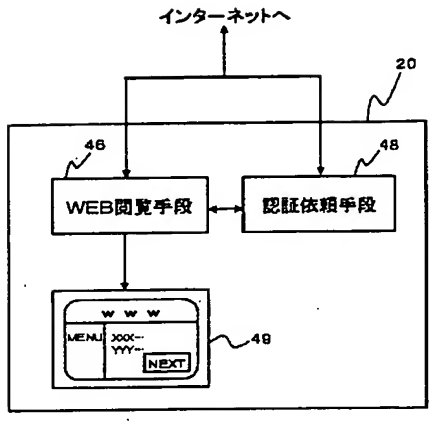
図4



【図５】

NCS－0023

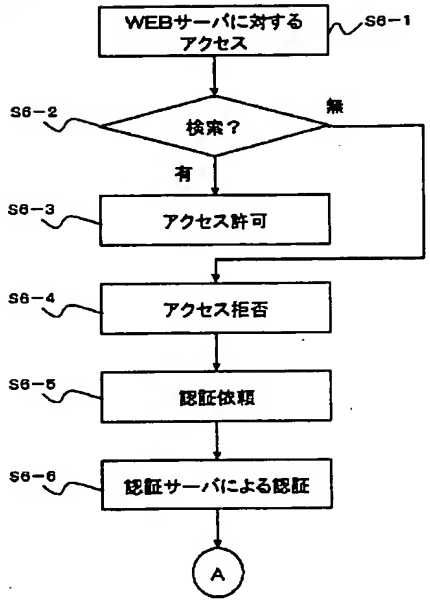
図5



【図６】

NCS－0023

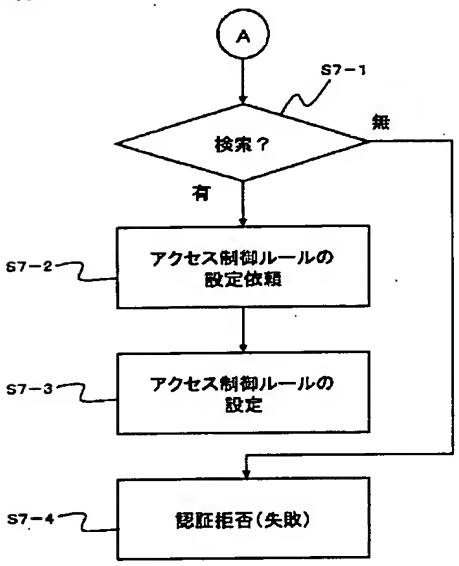
図6



【図７】

NCS－0023

図7



【図８】

NCS－0023

図8